



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/773,535

02/02/2001

Tony Hashem

52493.000152

6306

7590

01/31/2006

Jennifer A. Albert, Esq.  
Hunton & Williams  
Suite 1200  
1900 K Street, N.W.  
Washington, DC 20006

EXAMINER

KHOSHNOODI, NADIA

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	09/773,535		HASHEM ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Nadia Khoshnoodi		2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 1/9/2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-63,66-76 and 78 is/are pending in the application.
- 4a) Of the above claim(s) 64-65 and 77 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-63,66-76 and 78 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 February 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>4/1-9-2006</u> . | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

***Claim Rejections - 35 USC § 103***

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

II. Claims 1-2, 10-11, 13-14, 16-17, 19, 23-24, 26-29, 31, 34, 36-37, 47-49, 61-62, 66-67, 71-70, 74, 76, and 78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958, and further in view of Haff et al., US Pub. No. 2002/0184224.

As per claims 1 and 23:

Leveridge et al. substantially teach a method for placing a file in a destination based transmit folder, transmitting data comprising retrieving a file from a destination based transmit folder (page 22, lines 18-21), encrypting the file with an encryption process associated with the destination based transmit folder (page 22, lines 4-17), and transmitting the file to an outgoing folder for transmission to a destination, which is associated with the destination based transmit folder (page 22, lines 18-19 and page 24, lines 14-17 and fig. 9, element 124). Leveridge et al. further teach wherein the particular encryption process converts the file from one data set to an encrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed is encrypting the file with a particular encryption process including determining the particular encryption process by which the file is to be encrypted, the determining being based on what destination based transmit folder the file was retrieved from in

Art Unit: 2137

such a manner that the destination based transmit folder dictates the particular encryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to encrypt each of the files that are being transmitted based on the particular encryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can encrypt the file using the public key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claim 2 and 24:

Leveridge et al. and Haff et al. substantially teach the method of claims 1 and 23. Leveridge et al. teach the method further comprising retrieving the encryption process associated with the destination based transmit folder from an encryption database on page 21, line 4 to page 22, line 17 depicted as element 126 in fig. 9. Although the term "encryption database" is not used, it accomplishes the same goal thus is identical.

As per claim 10:

Leveridge et al. and Haff et al. substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising transmitting notification of encryption failure of the file to the destination if the file fails encryption. However, Leveridge et al. teach the method of requesting retransmission where errors have been found regarding the encryption key.

Art Unit: 2137

Furthermore, Leveridge et al. constantly reiterate sending and acknowledgement or error depending on the outcome of different processes, for example the pre-processor. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to transmit a notification of encryption failure of the file to the destination if the file fails encryption.

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leveridge et al. on page 10 lines, 17-19 and page 19, lines 26-28. Furthermore, page 24 lines 1-13 shows that it was possible to apply the method of notification used for the key to the process of encrypting the file because they both contain the encryption checksum.

As per claim 11:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 1. Leveridge et al. also substantially teach the use of directories for various purposes as seen on page 22, lines 18-28 in one instance. Not explicitly disclosed by either Leveridge et al. is the method further comprising moving the file to an error directory if the file fails the encryption process. However, the mere definition of “directory” discloses why a directory is used. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to move files failing encryption to a directory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the definition as found at the following online site,

[http://www.geek.com/glossary/glossary\\_search.cgi?d](http://www.geek.com/glossary/glossary_search.cgi?d)

Art Unit: 2137

and also available by typing the keyword in onelook.com and choosing the link TECHNICAL under the computing dictionary section. The definition, as viewed online, is pasted below:

**Directory** - The name for a logical container for files. Directories were devised to organize files. Without directories, all the files on your hard drive would be in one big listing. When you request a list of files from a computer, you generally only see the files within one directory. Directories can contain files and/or other directories. Nowadays, most operating systems are calling directories "folders," but we know what they really are.

As per claims 13 and 26:

Leveridge et al. and Haff et al. substantially teach the method of claims 1 and 23.

Leveridge et al. teach the method further comprising retrieving the file from the outgoing box (page 20, lines 11-13), transmitting the file to the destination (page 24, lines 17-22), and verifying receipt of the file at the destination (page 20, lines 13-16).

As per claim 14:

Leveridge et al. and Haff et al. substantially teach the method of claims 1 and 23.

Leveridge et al. teach the method wherein a user selects a file destination (page 21, lines 4-26) and places the file in the destination based transmit folder corresponding to the file destination (page 22, lines 26-28).

As per claim 16:

Leveridge et al. and Haff et al. substantially teach the method of claim 1. Leveridge et al. teach the method further comprising transmitting the encrypted file (page 23, line 27 – page 24, line 16).

As per claim 17:

Leveridge et al. and Haff et al. substantially teach the method of claim 1. Leveridge et al. teach the method further comprising transmitting the encrypted file over an insecure channel (page 2, line 27 - page 3, line 6).

As per claim 19:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 1 above. Not explicitly disclosed is the method further comprising generating a file notifying a recipient at the destination that the file is being transmitted. However, Leveridge et al. teach the method of transmitting an error message or acknowledgment to the sender depending on the status of the transmission. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to also send a notification to the destination so that the recipient is aware that the file has been transmitted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leveridge et al. on page 19, line 26 – page 20, line 3.

As per claims 27 and 47:

Leveridge et al. teach a method for receiving data comprising placing a file in a destination based received folder, retrieving the file from a destination based received folder (page 22, lines 22-28), decrypting the file with a decryption process associated with the destination based received folder (page 22, lines 4-17), and transmitting the file to an outgoing folder for access at a destination (page 22, lines 26-28). Leveridge et al. further teach wherein the particular decryption process converts the file from an encrypted data set to a decrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed is decrypting the file with a particular decryption process including determining the particular decryption process by which the file is to be decrypted, the determining being based on what destination based received folder the file was retrieved from in such a manner that the destination based received folder dictates the particular decryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Furthermore, Haff et al. teach that the decryption occurs in a similar manner. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to decrypt each of the files that are being transmitted based on the particular decryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can decrypt the file using the private key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claims 28 and 48:

Leveridge et al. and Haff et al. substantially teach the method of claims 27 and 47. Leveridge et al. teach the method further comprising retrieving the decryption process associated with the destination based received folder from a decryption database on page 21, line 4 to page 22, line 17 depicted as element 126 in fig. 9. Although the term "decryption database" is not used, it accomplishes the same goal thus is identical.

As per claims 29 and 49:

Leveridge et al. and Haff et al. substantially teach the method of claims 1 and 23.

Leveridge et al. teach the method further comprising verifying that the file has been decrypted (page 20, lines 16-19 and page 24, lines 10-13).

As per claim 31:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 27 and the method of verifying that the file has been decrypted as applied to claim 29. Leveridge et al. also substantially teach the use of directories for various purposes as seen on page 22, lines 18-28 in one instance. Not explicitly disclosed is the method further comprising moving the file to an error directory if the file fails the verification process.

However, the mere definition of "directory" discloses why a directory is used. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to move files failing verification to a directory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the definition as found at the following online site,

[http://www.geek.com/glossary/glossary\\_search.cgi?d](http://www.geek.com/glossary/glossary_search.cgi?d)

and also available by typing the keyword in onelook.com and choosing the link TECHNICAL under the computing dictionary section. The definition, as viewed online, is pasted below:

**Directory** - The name for a logical container for files. Directories were devised to organize files. Without directories, all the files on your hard drive would be in one big listing. When you request a list of files from a computer, you generally only see the files within one directory. Directories can contain files and/or other directories. Nowadays, most operating systems are calling directories "folders," but we know what they really are.

As per claim 34:

Art Unit: 2137

Leveridge et al. and Haff et al. substantially teach the method of claim 29. Leveridge et al. teach the method wherein transmitting the file to the outgoing folder comprises transmitting the verified file to the outgoing folder (page 24, line 10-16).

As per claim 36:

Leveridge et al. and Haff et al. substantially teach the method further comprising transmitting notification to the destination. Not explicitly disclosed is the method further comprising transmitting notification of decryption failure of the file to the destination if the file fails decryption. However, Leveridge et al. teach the method of transmitting notification of a successful decryption to the destination. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to also transmit a notification of decryption failure of the file to the destination if the file fails decryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leveridge et al. page 20, lines 8-13.

As per claim 37:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 27. Leveridge et al. also substantially teach the use of directories for various purposes as seen on page 22, lines 18-28 in one instance. Not explicitly disclosed is the method further comprising moving the file to an error directory if the file fails the decryption process. However, the mere definition of "directory" discloses why a directory is used. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to move files failing decryption to a

Art Unit: 2137

directory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the definition as found at the following online site,

[http://www.geek.com/glossary/glossary\\_search.cgi?d](http://www.geek.com/glossary/glossary_search.cgi?d)

and also available by typing the keyword in onelook.com and choosing the link TECHNICAL under the computing dictionary section. The definition, as viewed online, is pasted below:

**Directory** - The name for a logical container for files. Directories were devised to organize files. Without directories, all the files on your hard drive would be in one big listing. When you request a list of files from a computer, you generally only see the files within one directory. Directories can contain files and/or other directories. Nowadays, most operating systems are calling directories "folders," but we know what they really are.

As per claims 61 and 66:

Leveridge et al. substantially teach a method for receiving data comprising automatically placing received data in a destination based received folder (page 22, lines 22-25), automatically retrieving the file from a destination based received folder (page 22, lines 22-28 and page 24, 17-22), decrypting the file with a decryption process associated with the destination based received folder (page 22, lines 4-17), decrypting the data with the decryption process (page 22, lines 11-17), and transmitting the file to an outgoing folder for access at a destination (page 22, lines 26-28). Leveridge et al. further teach wherein the particular decryption process converts the file from an encrypted data set to a decrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed is automatically retrieving a decryption process associated with the destination based received folder, the retrieving including determining the particular decryption process including determining the particular decryption process by which the file is to

Art Unit: 2137

be decrypted, the determining being based on what destination based received folder the file was retrieved from in such a manner that the destination based received folder dictates the particular decryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Furthermore, Haff et al. teach that the decryption occurs in a similar manner. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to decrypt each of the files that are being transmitted based on the particular decryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can decrypt the file using the private key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claims 62 and 67:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data of claims 61 and 66. Furthermore, Leveridge et al. teach wherein the decryption process comprises a decryption key (page 19, lines 19-21).

As per claim 70:

Leveridge et al. and Haff et al. substantially teach a method for receiving data as applied to claim 66. Leveridge et al. further teach the method further comprising performing error processing on the data if the data fails decryption on page 19, line 26 – page 20, line 19 and page 24, lines 10-13. Here, error processing is fulfilled by retransmission of the data.

As per claim 71:

Leveridge et al. substantially teach a method for transmitting data comprising receiving data in a destination based transmit folder (page 22, lines 18-21) and automatically encrypting the data (page 19, lines 15-21) with an encryption method associated with the destination based transmit folder (page 22, lines 4-17). Additionally, Leveridge et al. also teach the method for an encryption database storing encryption methods, each encryption method associated with at least one destination based transmit folder (page 21, line 4 to page 22, line 17 depicted as element 126 in fig. 9). Although the term “encryption database” is not used, it accomplishes the same goal thus is identical. Furthermore, Leveridge et al. also teach a method for error processing on data failing encryption on page 19, line 26 – page 20, line 19. Here, error processing is fulfilled by retransmission of the data. Leveridge et al. further teach wherein the particular encryption process converts the file from one data set to an encrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed by Leveridge et al. et al. is an encryption module and an error module. However, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate an encryption module to receive data in a destination based transmit folder to encrypt and an error module to perform the error processing on data failing encryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

Art Unit: 2137

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

Also not explicitly disclosed is encrypting the file with a particular encryption process including determining the particular encryption process by which the file is to be encrypted, the determining being based on what destination based transmit folder the file was retrieved from in such a manner that the destination based transmit folder dictates the particular encryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to encrypt each of the files that are being transmitted based on the particular encryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can encrypt the file using the public key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claim 74:

Leveridge et al. substantially teach a method for receiving data comprising receiving data in a destination based received folder (page 22, lines 22-28) and automatically decrypting the data (page 19, lines 15-21) with a decryption method associated with the destination based received folder (page 22, lines 4-17). Additionally, Leveridge et al. also teach the method for an

Art Unit: 2137

decryption database storing encryption methods, each decryption method associated with at least one destination based received folder (page 21, line 4 to page 22, line 17 depicted as element 126 in fig. 9). Although the term “decryption database” is not used, it accomplishes the same goal thus is identical. Furthermore, Leveridge et al. also teach a method for error processing on data failing decryption on page 19, line 26 – page 20, line 19 and page 24, lines 10-13. Here, error processing is fulfilled by retransmission of the data. Leveridge et al. further teach wherein the particular decryption process converts the file from an encrypted data set to a decrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed by Leveridge et al. et al. is a decryption module and an error module. However, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a decryption module to receive data in a destination based transmit folder to decrypt and an error module to perform the error processing on data failing decryption. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

Not explicitly disclosed is automatically retrieving a decryption process associated with the destination based received folder, the retrieving including determining the particular

Art Unit: 2137

decryption process including determining the particular decryption process by which the file is to be decrypted, the determining being based on what destination based received folder the file was retrieved from in such a manner that the destination based received folder dictates the particular decryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Furthermore, Haff et al. teach that the decryption occurs in a similar manner. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to decrypt each of the files that are being transmitted based on the particular decryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can decrypt the file using the private key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claim 76:

Leveridge et al. and Haff et al. substantially teach the method, as applied to claim 74 above, for verifying that the data has been decrypted (page 20, lines 16-19 and page 24, lines 10-13). Not explicitly disclosed is a verification module performing the verification within a decryption module. However, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a verification module to verify that the decryption was successful. This modification would have been obvious because a

Art Unit: 2137

person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

As per claim 78:

Leveridge et al. and Haff et al. substantially teach the method of claim 1. Furthermore, Haff et al. teach wherein the determining is performed after the file is retrieved from the destination base transmit folder (par. 169).

III. Claims 3, 5, 8, 20-22, 25, 40-42, 44-46, 50-52, 54-57, 72-73, and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958 as previously applied to claims 1 (for claims 3 and 20-22), 23 (for claim 25), 27 (for claims 40-42 and 44-46), 47 (for claim 50), 71 (for claims 72-73), and 74 (for claim 75) and Haff et al., US Pub. No. 2002/0184224, and further in view of Ote et al. United States Patent No. 6,023,506.

As per claims 3 and 25:

Leveridge et al. and Haff et al. substantially teach a method of transmitting data as in claims 1 and 23. Not explicitly disclosed is the method further comprising verifying that the file has been encrypted. However, Ote et al. teach the method further comprising verifying that the file has been encrypted. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to verify that the file was indeed encrypted. This modification would have been obvious because

Art Unit: 2137

a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. by fig. 8, element 6007.

As per claim 5:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 1. Ote et al. substantially teach the method of verifying that the file has been encrypted as applied to claim 3. Leveridge et al. and Ote et al. also substantially teach the use of directories for various purposes as seen on page 22, lines 18-28 in an instance of Leveridge et al. and col. 4, lines 41-46 in an instance of Ote et al. Not explicitly disclosed is the method further comprising moving the file to an error directory if the file fails the verification process.

However, the mere definition of "directory" discloses why a directory is used. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step to move files failing verification to a directory. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the definition as found at the following online site,

[http://www.geek.com/glossary/glossary\\_search.cgi?d](http://www.geek.com/glossary/glossary_search.cgi?d)

and also available by typing the keyword in onelook.com and choosing the link TECHNICAL under the computing dictionary section. The definition, as viewed online, is pasted below:

**Directory** - The name for a logical container for files. Directories were devised to organize files. Without directories, all the files on your hard drive would be in one big listing. When you request a list of files from a computer, you generally only see the files within one directory. Directories can contain files and/or other directories. Nowadays, most operating systems are calling directories "folders," but we know what they really are.

As per claim 8:

Leveridge et al. and Haff et al. substantially teach the method of transmitting data as applied to claim 1. Ote et al. substantially teach the method of verifying that the file has been encrypted as applied to claim 3. Not explicitly disclosed is the method wherein transmitting the file to the outgoing folder comprises transmitting the verified file to the outgoing folder. However, Leveridge et al. disclose this method when dealing with decryption. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step to transmit the verified file to the outgoing folder. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leveridge et al. on page 24, line 10-16.

As per claims 20 and 44:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as in claims 1 and 27. Not explicitly disclosed is the method further comprising performing a scan for encryption key software to find the encryption process. However, Ote et al. teach the method for using an encryption/decryption software for the encryption/decryption process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to store the encryption/decryption software in the database from which the encryption/decryption process is chosen. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. column 14, line 27 – col. 15, line 9.

As per claim 21:

Leveridge et al. and Haff et al. substantially teach a method for transmitting data comprising transmitting a file from the destination based transmit folder to the outgoing folder to reconcile a file being transferred from the destination based transmit folder to the outgoing folder as applied to claim 1. Not explicitly disclosed is transmitting a list of files. However, Ote et al. teach the method further comprising transmitting a list of files. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to allow transmission of a list of files as opposed to a single file. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

As per claim 22:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as in claim 1. Not explicitly disclosed is the method further comprising compressing the data. However, Ote et al. teach a method of compressing data. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a method of compressing data before the encryption takes place. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

As per claims 40 and 50:

Leveridge et al. and Haff et al. substantially teach a method for receiving data as applied to claims 27 and 47. Leveridge et al. teach the method further comprising receiving the file in a

Art Unit: 2137

file received outbox (fig. 9, element 124). Not explicitly disclosed is transmitting data comprising receiving the file in a file received inbox and placing the file in the destination based received folder. However, Ote et al. teach the method further comprising receiving the file in a file received inbox and placing the file in the destination based received folder. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to receive the file in the recipient's inbox then place it in the destination based received folder, which as previously stated is associated with the decryption process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 12, line 60 – col. 13, line 19.

As per claim 41:

Leveridge et al. and Haff et al. substantially teach a method as applied to claim 40. Leveridge et al. teach the method further comprising receiving the file over an insecure channel (page 2, line 27 - page 3, line 6). Although it doesn't say "receiving," transferring from one client to another implies that the second client is receiving.

As per claim 42:

Leveridge et al. and Haff et al. substantially teach a method as applied to claim 41. Leveridge et al. teach the method wherein placing the file in the appropriate destination based received folder comprises determining destination of the file on page 22, lines 22-25.

As per claim 45:

Leveridge et al. and Haff et al. substantially teach a method for transmitting data comprising transmitting a file from the destination based received folder to the outgoing folder to

Art Unit: 2137

reconcile a file being transferred from the destination based received folder to the outgoing folder as applied to claim 1. Not explicitly disclosed is transmitting a list of files. However, Ote et al. teach the method further comprising transmitting a list of files. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to allow transmission of a list of files as opposed to a single file. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

As per claim 46:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as in claim 27. Not explicitly disclosed is the method further comprising decompressing the data. However, Ote et al. teach a method of decompressing data. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a method of decompressing data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

As per claims 51 and 56:

Leveridge et al. substantially teach a method for transmitting data comprising placing a file in a destination based transmit folder, retrieving a file from a destination based transmit folder (page 22, lines 18-21), encrypting the file with an encryption process associated with the destination based transmit folder (page 22, lines 4-17), encrypting the data with the encryption

Art Unit: 2137

process (depicted in fig. 14; page 22, lines 9-17) and transmitting the file to an outgoing folder for transmission to a destination (page 24, lines 14-17 and fig. 9, element 124). Leveridge et al. further teach wherein the particular encryption process converts the file from one data set to an encrypted data set, access to the file being precluded while the file is encrypted (page 25, line 19 – page 26, line 10).

Not explicitly disclosed by Leveridge et al. is the method automatically retrieving data from a destination based transmit folder or automatically retrieving an encryption process associated with the destination based transmit folder. However, Leveridge et al. teach a method for each recipient maintaining an updated directory. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to use this automatic update feature to allow for an automatic method of data retrieval from a destination based transmit folder. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leveridge et al. on page 24, lines 17-22.

As for automatically retrieving an encryption process, Ote et. al teach that. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to use this automatic encryption process associated with the destination based transmit folder as previously discussed. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 1, line 33 – col.2, line 6.

Finally, not explicitly disclosed is the retrieving including determining the particular encryption process by which the data is to be encrypted, the determining being based on what destination based transmit folder the file was retrieved from in such a manner that the destination based transmit folder dictates the particular encryption process. However, Haff et al. teach that when encryption is used within the system, there is a particular public key code that is linked to the destination address of the user's terminal that is receiving the file. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to encrypt each of the files that are being transmitted based on the particular encryption key associated with the user's terminal where the file will ultimately be received. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Haff et al. suggest that the user can encrypt the file using the public key of the public/private key pair so that the correct user gains access to the information in the file in paragraph 169.

As per claims 52 and 57:

Leveridge et al., Haff et al., and Ote et al. and substantially teach the method for transmitting data as in claims 51 and 56. Leveridge et al. further teach the method wherein the encryption process comprises an encryption key (page 19, lines 19-21).

As per claims 54 and 55:

Leveridge et al., Haff et al., and Ote et al. and substantially teach the method for transmitting data as in claim 51. Furthermore, Leveridge et al. teach the method further comprising performing error processing on the data if the data fails verification or encryption on

Art Unit: 2137

page 19, line 26 – page 20, line 19. Here, error processing is fulfilled by retransmission of the data.

As per claim 72:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as applied to claim 71 above. Not explicitly disclosed is the method further comprising compressing the data. However, Ote et al. teach a method of compressing data. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a method of compressing data before the encryption takes place. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

Furthermore, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a compression module to compress the data to be transmitted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

As per claim 73:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as applied to claim 71 above. Not explicitly disclosed is the encryption module comprising a verification module verifying encryption of the data. However, Ote et al. substantially teach the method for verifying encryption of the data. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to verify that the file was indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. by fig. 8, element 6007.

Furthermore, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a verification module to verify that the encryption was successful. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

As per claim 75:

Leveridge et al. and Haff et al. substantially teach the method for transmitting data as applied to claim 74 above. Not explicitly disclosed is the method further comprising

Art Unit: 2137

decompressing the received data. However, Ote et al. teach a method of decompressing data.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a method of decompressing data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ote et al. in col. 7, lines 15-21.

Furthermore, a module is merely a part of a program that performs a particular task. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a decompression module to compress the data to be transmitted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by the following definition of module found online at:

<http://www.computeruser.com/resources/dictionary>

The definition, as viewed online, is pasted below:

Module- A self-contained functional unit which is used with a larger system. A software module is a part of a program that performs a particular task. A hardware module can be a packaged unit that attaches to a system.

IV. Claims 4, 53, and 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958, Haff et al., US Pub. No. 2002/0184224, and Ote et al. United States Patent No. 6,023,506 as applied to claims 3, 51, and 56 above, and further in view of Brundrett et al. United States Patent No. 6,249,866.

As per claim 4:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method for transmitting data as applied to claim 1. Ote et al. substantially teach the method of verifying that the file has been encrypted as applied to claim 3. Not explicitly disclosed is the method of verifying that the file has been encrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted. However, Brundrett et al. teach the method of transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method consists of transferring the file, they do disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Furthermore, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212.

As per claim 53:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method for transmitting data as applied to claim 51. Not explicitly disclosed is the method of verifying that the file has been encrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted. However, Brundrett et al. teach the method of

Art Unit: 2137

transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method consists of transferring the file, they do disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Furthermore, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212.

As per claim 58:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method for transmitting data as applied to claim 56. Not explicitly disclosed is the method of verifying that the file has been encrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted. However, Brundrett et al. teach the method of transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method consists of transferring the file, they do disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Furthermore, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212.

As per claims 59-60:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method for transmitting data as applied to claim 56. Brundrett et al. substantially teach the method of transferring the data to a temporary folder for verification as applied to claim 58. Furthermore, Leveridge et al. teach the method further comprising performing error processing on the data if the data fails verification on page 19, line 26 – page 20, line 19. Here, error processing is fulfilled by retransmission of the data.

V. Claims 6, 7, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958, Haff et al., US Pub. No. 2002/0184224, and Ote et al. United States Patent No. 6,023,506 as applied to claim 3 (for 6 and 9) above and 6 (for claim 7) below and further in view of Lockhart et al. United States Patent No. 5,841,873.

As per claim 6:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method as in claim 3. Not explicitly disclosed is that method further comprising recording information about the file in an

error log if the file fails the verification process. However, Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the verification process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step to record information about the file in an error log if the file fails the verification process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61.

As per claim 7:

Leveridge et al., Haff et al., Ote et al., and Lockhart et al. substantially teach a method as in claim 3 above. Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the verification process as applied to claim 6 above. Not explicitly disclosed is the method further comprising transmitting a destination based portion of the error log to the destination. However, Lockhart et al. teach the method further comprising generating an error report message which is recorded in an error log and transmitted. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step to transmit a portion of the error log to the destination once the error log was recorded after the failed verification process.

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61. Furthermore, although Lockhart et al. do not explicitly state that the generated error message is being transmitted to the destination,

it is transmitted to a server, thus the modification of sending the destination based portion of the error log to element SFTS, in fig. 9 of Leveridge et al. for the server to put in the recipient outbox for retrieval at the destination would have also been obvious.

As per claim 9:

Leveridge et al., Haff et al., and Ote et al. substantially teach a method as in claim 3 above. Not explicitly disclosed is that method further comprising transmitting notification of verification failure of the file to the destination if the file fails verification. However, Lockhart et al. teach the method further comprising transmitting notification of verification failure if the file fails the verification process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step to send a notification of verification failure if the file fails the verification process.

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61. Furthermore, the modification of sending the notification of the failed verification process to the destination would have been obvious because of how the method for transmitting data is disclosed in Leveridge et al. and the verification process is disclosed in Ote et al. Also, the modification would only require adding a single step for notification if the file failed verification, i.e. when the result to element 6007 of fig. 8 in Ote et al. is no, there could be a step directly following to send notification.

VI. Claims 15 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958 and Haff et al., US Pub. No. 2002/0184224, as applied to claims 1 and 27 above and further in view of Berman et al. United States Patent No. 5,995,939.

Art Unit: 2137

As per claim 15:

Leveridge et al. and Haff et al. substantially teach a method of transmitting data as applied to claim 1. Leveridge et al. also substantially teach the method for each recipient keeping an updated destination based transmit folder for retrieving files on page 24, lines 17-22. Not explicitly disclosed is the method for automatically checking the destination based transmit folder for new files after a predetermined time interval. However, Berman et al. teach a method for automatically checking for new files after a predetermined time interval. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to retrieve new files found in the updated directory after a predetermined time interval. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Berman et al. in col. 6, line 28 – col. 7, line 44.

As per claim 39:

Leveridge et al. and Haff et al. substantially teach a method of receiving data as applied to claim 27. Leveridge et al. also substantially teach the method for each recipient keeping an updated destination based received folder for retrieving files on page 24, lines 17-22. Not explicitly disclosed is the method for automatically checking the destination based received folder for new files after a predetermined time interval. However, Berman et al. teach a method for automatically checking for new files after a predetermined time interval. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to retrieve new files found in the updated directory after a predetermined time interval. This modification would have been obvious because a person

Art Unit: 2137

having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Berman et al. in col. 6, line 28 – col. 7, line 44.

VII. Claims 18, 30, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958 and Haff et al., US Pub. No. 2002/0184224, as applied to claims 1, 29, and 27 above and further in view of Brundrett et al. United States Patent No. 6,249,866.

As per claim 18:

Leveridge et al. and Haff et al. substantially teach a method of transmitting data as in claim 1. Not explicitly disclosed is that method wherein the encryption process comprises a public key for encoding the file. However, Brundrett et al. teach the method wherein the encryption process comprises a public key for encoding the file. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to encrypt the file with a public key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 9, lines 64-66.

As per claim 30:

Leveridge et al. and Haff et al. substantially teach the method of verifying that the file has been decrypted as in claim 29. Not explicitly disclosed is the method of verifying that the file has been decrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been decrypted. However, Brundrett et al. teach the method of transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method

Art Unit: 2137

consists of transferring the file, they do disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones.

Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Ote et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Also, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212. Furthermore, Brundrett et al. disclosed a method for encryption thus it is obvious for use in decryption as well since decryption is the “converse operation” of encryption as stated in col. 18, lines 17-19.

As per claim 43:

Leveridge et al. and Haff et al. substantially teach a method of transmitting data as in claim 27. Not explicitly disclosed the method wherein the decryption process comprises a private key for decoding the file. However, Brundrett et al. teach the method wherein the decryption process comprises a private key for decoding the file. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to decrypt the file with a private key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 9, lines 64-66.

Art Unit: 2137

VIII. Claims 12, 32-33, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958 and Haff et al., US Pub. No. 2002/0184224, as applied to claims 1, 29, and 27 above and further in view of Lockhart et al. United States Patent No. 5,841,873.

As per claim 12:

Leveridge et al. and Haff et al. substantially teach a method for transmitting data as in claim 1. Not explicitly disclosed is the method further comprising recording information about the file in an error log if the file fails the encryption process. However, Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the encryption process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to record information about the file in an error log if the file fails the encryption process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61.

As per claim 32:

Leveridge et al. and Haff et al. substantially teach a method for verifying that the file has been decrypted as in claim 29. Not explicitly disclosed is the method further comprising recording information about the file in an error log if the file fails the verification process. However, Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the verification process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to record information about the file in an error log if the file

Art Unit: 2137

fails the verification process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61.

As per claim 33:

Leveridge et al. and Haff et al. substantially teach a method for transmitting data and verifying that the decryption has been verified as applied to claim 29 above. Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the verification process as applied to claim 32 above. Not explicitly disclosed is the method further comprising transmitting a destination based portion of the error log to the destination.

However, Lockhart et al. teach the method further comprising generating an error report message which is recorded in an error log and transmitted. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to transmit a portion of the error log to the destination once the error log was recorded after the failed verification process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61. Furthermore, although Lockhart et al. do not explicitly state that the generated error message is being transmitted to the destination, it is transmitted to a server, thus the modification of sending the destination based portion of the error log to element SFTS, in fig. 9 of Leveridge et al. for the server to put in the recipient outbox for retrieval at the destination would have also been obvious.

As per claim 38:

Leveridge et al. and Haff et al. substantially teach a method for verifying that the file has been decrypted as in claim 27. Not explicitly disclosed is the method further comprising recording information about the file in an error log if the file fails the decryption process. However, Lockhart et al. teach the method further comprising recording information about the file in an error log if the file fails the decryption process. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step to record information about the file in an error log if the file fails the decryption process. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lockhart et al. in col. 6, lines 9-32 and col. 2, lines 58-61.

IX. Claims 63 and 68-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leveridge et al. WO 99/00958 and Haff et al. United States Pub. No. 2002/0184224 as applied to claims 61 and 66 above, and further in view of Brundrett et al. United States Patent No. 6,249,866.

As per claim 63:

Leveridge et al. and Haff et al. substantially teach the method of receiving data as applied to claim 61. Not explicitly disclosed by Leveridge et al. or Ote et al. is the method of verifying that the file has been decrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been decrypted.

However, Brundrett et al. teach the method of transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method consists of transferring the file, they do

Art Unit: 2137

disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Also, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212. Furthermore, Brundrett et al. disclosed a method for encryption thus it is obvious for use in decryption as well since decryption is the “converse operation” of encryption as stated in col. 18, lines 17-19.

As per claim 68:

Leveridge et al. and Haff et al. substantially teach the method of receiving data as applied to claim 66. Not explicitly disclosed is the method of verifying that the file has been decrypted comprises transferring the file to a temporary folder and checking if all files in the temporary folder have been decrypted.

However, Brundrett et al. teach the method of transferring the file to a temporary folder and checking if all files in the temporary folder have been encrypted to verify the encryption. Although Brundrett et al. do not state that their method consists of transferring the file, they do disclose the method of creating a new temporary file and copying the attributes from the originals to the temporary ones. Therefore, it would have been obvious to a person in the art at

Art Unit: 2137

the time the invention was made to modify the method disclosed in Leveridge et al. to incorporate a step into the verification of encryption to transfer the file to a temporary folder and check that they were indeed encrypted. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Brundrett et al. in col. 18, lines 50-56. Also, it would have been obvious to check the temporary files for verifying the encryption because it is suggested that Brundrett et al. verify the success in col. 18, lines 6-12 and in fig. 22, element 2212. Furthermore, Brundrett et al. disclosed a method for encryption thus it is obvious for use in decryption as well since decryption is the “converse operation” of encryption as stated in col. 18, lines 17-19.

As per claim 69:

Leveridge et al. and Haff et al. substantially teach a method for receiving data as applied to claim 66. Brundrett et al. substantially teach the method of transferring the data to a temporary folder to verify decryption as applied to claim 68. Leveridge et al. teach the method further comprising performing error processing on the data if the data fails verification on page 19, line 26 – page 20, line 19 and page 24, lines 10-13. Here, error processing is fulfilled by retransmission of the data.

*Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Nadia Khoshnoodi  
Examiner  
Art Unit 2137  
1/19/2006

NK



EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER